UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,314	02/26/2004	Brig Barnum Elliott	BBNT-P01-265	3449

28120 7590 05/08/2007

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,314	ELLIOTT, BRIG BARNUM	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :2/26/04; 2/2/06; 7/20/06; 11/15/06; 1/22/07.

DETAILED ACTION

1. Claims 1-37 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 26 February 2004, 02 February 2006, 20 July 2006, 15 November 2006, and 22 January 2007 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statements.

Drawings

3. Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the subject matter in claim 32, specifically the machine-readable medium. The Applicant does not define a computer-readable medium, and therefore renders it impossible to ascertain the intended scope of the claim. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 6-11 provides for the use of the cryptographic key material, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 2-11 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd. App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

9. Claim 32 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. One of ordinary skill in the art could conclude that the claimed machine-readable medium of claim 32 is a transmission medium, carrier wave, or something of the like since the Applicant discloses that the invention is at least used in a networking environment on at least page 4. The Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

10. Claim 33 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As per claim 33, merely claimed as means for where the means is implemented in software representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process, as there are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program's functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program's functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

11. Page 26, paragraph 0072 of the Specification of the instant application describes that the present invention can be implemented as software, thereby rendering the "means for" language in claim 33 as computer software. *In re Donaldson Co.*, 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), decided that

> the "broadest reasonable interpretation" that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination.

See MPEP § 2181 also. Therefore, giving the claims their broadest reasonable interpretation, while keeping the structure disclosed in the specification in my mind, one of ordinary skill in the art would construe claim 33 as representing a computer program *per se*.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1, 2, 6-15, and 17-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0036624 to Kent et al., hereinafter Kent, in view of U.S. Patent No. 6,661,806 to Eriksson et al., hereinafter Ericksson.

14. As per claims 1 and 31-34, Kent teaches a key agreement protocol in a quantum communication environment wherein a sender transmits binary strings to a receiver and from there the receiver creates a random cryptographic key using the binary strings (Abstract, paragraph 0014).

15. Kent does not teach wherein the receiver requests a certain rate of transfer for the data, the sender determining if it can provide that service to recipient, and, upon determining it can, guaranteeing said transfer rate.

16. Ericksson teaches resource reservation, specifically guaranteeing data flow (column 2, lines 33-54) and guaranteeing that services to end users (column 2, lines 59-65).

17. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the resource reservation and quality of service guarantee of

Ericksson in the quantum key distribution of Kent, since Ericksson states at column 1, lines 17-21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data which would be important in a key agreement protocol similar to the one disclosed by the Kent reference.

18. Regarding claim 2, Kent teaches wherein the secret bits are cryptographic key material (paragraph 0003).

19. With regards to claims 6-10, Kent teaches a communication network (Figure 1 [block 16]), which includes using the cryptographic key material to protect traffic flows through an Ethernet network, an internet, an ATM network, a Synchronous Optical Network (SONET), and Multiprotocol label switching networks, and Official Notice of such is herein taken. U.S. Patent Application No. 2003/0215088 to Bao provides extrinsic evidence, illustrating a similar system, while paragraphs 0083-0116 specifically disclose the various networks that such systems embody.

20. With regards to claim 11, Kent teaches using the cryptographic key material to provide secure communications (paragraph 0030).

21. With regards to claim 12, Kent teaches wherein the first secret bits producing application is based on advantage distillation (paragraph 0028), wherein the Examiner interprets advantage distillation as minimizing the eavesdropper's knowledge of the key.

22. With regards to claim 13, Kent teaches wherein the secret bit producing application is included in a quantum cryptographic system (paragraph 0017).

23. Concerning claims 14 and 15, Kent teaches wherein the quantum cryptographic system employs a laser or a photon source (paragraph 0049).

24. Concerning claim 17, Kent teaches wherein the quantum cryptographic system employs a phase/polarization modulator (paragraphs 0024, 0050).

25. Concerning claims 18 and 19, Kent teaches wherein the quantum cryptographic system employs a free space optical path or an optical fiber path (paragraph 0009).

26. Concerning claim 20, Kent teaches wherein the quantum cryptographic system employs a link comprising photonic band-gap material (Figure 5, paragraphs 0057-0061).

27. Regarding claim 21, Ericksson teaches sending a second reservation request for reserving a second rate from a second secret bit consuming application to the secret bits producing application, wherein the first reservation request and the second reservation request each include a priority of the respective request and the second reservation request has a different priority than the first reservation request (column 6, lines 28-47, column 3, lines 48-62).

28. Regarding claim 22, Kent teaches using secret bits from the secret bits producing application by a second secret bits consuming application having no requested reserved rate (paragraph 0014).

29. Regarding claim 23, Ericksson teaches wherein the reservation request includes a priority (column 1, lines 32-38, column 3, lines 48-62), a desired rate, and a minimum acceptable bit rate (column 5, lines 41-48).

30. With regards to claim 24, Ericksson teaches wherein the reserving the first rate comprises:

determining, by the secret bit producing application, whether the desired rate can be satisfied (column 2, lines 33-54, column 2, lines 59-65);

when the desired rate can be satisfied, sending a reply message to the requesting secret bit consuming application indicating a full-success (column 10, lines 12-41, i.e. accepting reservation);

when the desired rate cannot be satisfied, sending a reply message to the requesting secret bit consuming application indicating a partial-success when an amount of available of the rate is at least enough to satisfy the minimum acceptable rate (column 10, lines 12-51, i.e. rejecting reservation request); and

sending a reply message to the requesting secret bit consuming application indicating a failure to reserve the first rate when neither the desired rate nor the minimum acceptable rate can be satisfied (column 10, lines 12-51, i.e. rejecting reservation request).

31. Regarding claim 25, Ericksson teaches canceling a reservation when the secret bits producing application receives a message from the secret bits consuming application indicating that a reservation of the first rate is no longer needed by the secret bits consuming application (column 5, lines 10-17).

32. Regarding claim 26, Kent teaches determining an estimated bit production rate by the secret bits producing application (paragraph 0017).

33. With regards to claim 27, Kent teaches calculating an available rate of secret bits available for reservations, the calculating comprising calculating a total number of secret bits reserved for a secret bits consuming application; and subtracting the total number of secret bits reserved for a secret bits consuming application from the estimated bit production rate to produce the available rate of secret bits available for reservations (paragraph 0014).

34. Concerning claim 28, Ericksson teaches deleting at least one lowest priority reservation when the available rate of secret bits becomes negative, the deleting continuing until the available rate of secret bits becomes non-negative (column 5, lines 10-22).

35. Regarding claim 29, Kent teaches issuing a warning, by the secret bits producing application, when use of secret bits by the first secret bits consuming application from the secret bits producing application exceeds the first rate reserved for the first secret bits consuming

application (paragraphs 0011, 0014, i.e. eavesdropper does not know the correct bit and therefore would use too many).

36. Regarding claim 30, Ericksson teaches wherein the reserving act reserves the first rate for a limited period of time (column 4, lines 57-67).

37. As per claim 35, Kent teaches a key agreement protocol that is based on advantage distillation (Abstract, paragraph 0014, paragraph 0028), wherein the Examiner interprets advantage distillation as minimizing the eavesdropper's knowledge of the key.

38. Kent does not specifying a desired rate by a first process; and reserving the desired rate by the secret bit producer that is based on advantage distillation.

39. Ericksson teaches resource reservation, specifically guaranteeing data flow (column 2, lines 33-54) and guaranteeing that services to end users (column 2, lines 59-65).

40. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the resource reservation and quality of service guarantee of Ericksson in the quantum key distribution of Kent, since Ericksson states at column 1, lines 17-21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data which would be important in a key agreement protocol similar to the one disclosed by the Kent reference.

41. As per claim 36, Kent teaches a key agreement protocol that is based on advantage distillation (Abstract, paragraph 0014, paragraph 0028), wherein the Examiner interprets advantage distillation as minimizing the eavesdropper's knowledge of the key.

42. Kent does not teach receiving a request from a secure communication process for a reservation of the cryptographic key material at a first rate, the request identifying a minimum acceptable rate; and notifying the secure communication process of a successful reservation when an available generated rate of cryptographic key material is greater than the minimum acceptable rate.

43. Ericksson teaches resource reservation, specifically guaranteeing data flow (column 2, lines 33-54) and guaranteeing that services to end users (column 2, lines 59-65).

44. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the resource reservation and quality of service guarantee of Ericksson in the quantum key distribution of Kent, since Ericksson states at column 1, lines 17-21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data which would be important in a key agreement protocol similar to the one disclosed by the Kent reference.

45. As per claim 37 Kent teaches a key agreement protocol in a quantum communication environment wherein a sender transmits binary strings to a receiver and from there the receiver creates a random cryptographic key using the binary strings (Abstract, paragraph 0014).

46. Kent does not teach specifying a minimum desired consumption rate of secret key material and a priority by a client process; determining, by a secret key material producing

process, whether the minimum desired consumption rate of secret key material is available to the client process; when the minimum desired consumption rate of secret key material is not available to the client process, making at least the minimum desired consumption rate of secret key material available by canceling at least one previously made reservation of a rate of the secret key material, each of the at least one previously made reservation having a lower priority than the specified priority; and reserving at least the minimum desired consumption rate of the secret key material for the client process.

47. Ericksson discloses specifying a minimum desired consumption rate of data and a priority by a client process (column 1, lines 32-38, column 3, lines 48-62, column 4, line 57 to column 5, line 2);

determining whether the minimum desired consumption rate of data is available to the client process (column 2, lines 33-54, column 2, lines 59-65);

when the minimum desired consumption rate of data is not available to the client process, making at least the minimum desired consumption rate of data available by canceling at least one previously made reservation of a rate of the data, each of the at least one previously made reservation having a lower priority than the specified priority (column 10, lines 12-51, column 9, Table 2, i.e. rejecting reservation request or lowering priority); and

reserving at least the minimum desired consumption rate of the data for the client process (column 6, lines 10-47).

48. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the resource reservation and quality of service guarantee of Ericksson in the quantum key distribution of Kent, since Ericksson states at column 1, lines 17-

21 that guaranteeing a level of service ensures the appropriate bandwidth availability, thereby preventing the delay and loss of data which would be important in a key agreement protocol similar to the one disclosed by the Kent reference.

49. Claims 3-5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent in view of Ericksson as applied above, and in further view of U.S. Patent Application Publication No. 2001/0038695 to Kim, hereinafter Kim.

50. With regards to claim 3, Kent does not teach wherein the secret bit producing application is included in a system receiving random or pseudo-random sequences from an external source.

51. Kim teaches wherein the secret bit producing application is included in a system receiving random or pseudo-random sequences from an external source (paragraph 0024).

52. It would have been obvious to one of ordinary skill in the art at the time the invention was made to produce the secret bits using pseudo-random sequences, since Kim states at paragraph 0025 that using a pseudo-random sequence allows the users to exchange data without installing any additional security equipment, thereby making it easier to implement in various types of communication systems.

53. Concerning claim 4, Kim teaches wherein the system is implemented in any communication system (paragraph 0025), which includes systems where the external source is a satellite and Official Notice is taken of such.

54. Concerning claim 5, Kent teaches wherein the random or the pseudo-random sequences are transmitted via radio-frequency signals (paragraphs 0009, 0043).

55. Concerning claim 16, Kent does not teach a Mach-Zehnder interferometer.

56. Kim teaches a Mach-Zehnder interferometer (paragraphs 0035, 0038).

57. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include an interferometer in the quantum key distribution system, since Kim states at paragraph 0035 that an interferometer can cause time delay or filter certain frequencies in order to determine the coherent interference between the pulses (paragraph 0038).

Conclusion

58. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

59. The following patents are cited to further show the state of the art with respect to quantum key distribution, such as:

United States Patent Application Publication No. 2003/0215088 to Bao, which is cited to show a key agreement protocol based on network dynamics, such as error rate or transmission rate.

United States Patent Application Publication No. 2003/0137944 to Medvinsky, which is cited to show authenticating a quality of service reservation.

United States Patent Application Publication No. 2003/0002670 to Wang, which is cited to show a quantum cryptographic communication channel with a quantum conference or key agreement protocol.

United States Patent No. 6,522,749 to Wang, which is cited to show a quantum cryptographic communication channel with a quantum conference or key agreement protocol.

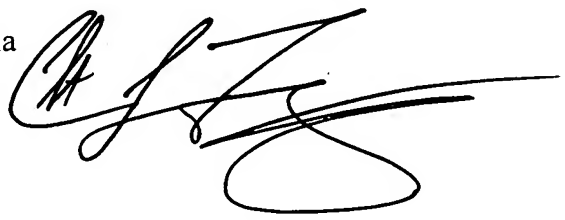
United States Patent Application Publication No. 2006/0252381 to Sasaoka et al., which is cited to show a key agreement protocol in a radio communication system.

60. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

61. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

62. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131



clf